WHAT IS CLAIMED IS:

1. A method of creating and maintaining a centralized key store comprising:

providing at least one security policy, wherein each security policy includes an application instance identifier associated with a security service; and

creating at least one security association, wherein the at least one security association is created based upon the security service associated with the application instance identifier to thereby create a centralized key store including the at least one security policy and at least one security association.

2. A method according to Claim 1 further comprising:

receiving at least one packet of data; and

applying the security service associated with the application instance identifier to the at least one packet of data to thereby transform the at least one packet of data, wherein the security service is applied to the at least one packet based upon the at least one security policy and the at least one security association.

3. A method according to Claim 2 further comprising:

receiving the at least one transformed packet of data; and

applying the security service associated with the application instance identifier to the at least one transformed packet of data to thereby generate a representation of the at least one packet of data, wherein the security service is applied to the transformed at least one packet based upon the at least one security association.

4. A method according to Claim 2, wherein providing at least one security policy comprises providing at least one security policy further including at least one selector field having at least one selector value in a format common to a plurality of security service protocols, and wherein applying the security service comprises applying the security service further based upon the at least one security policy including the at least one selector value.

5. A method according to Claim 1, wherein creating at least one security association comprises creating at least one security association according to an Internet Key Exchange (IKE) technique.

6. A system for creating and maintaining a centralized key store comprising:

a first security gateway capable of applying a security service associated with an application instance identifier to at least one packet of data to thereby transform the at least one packet of data, wherein the first security gateway is capable of applying the security service to the at least one packet based upon at least one security policy and at least one security association; and

a second security gateway capable of applying the security service associated with the application instance identifier to the at least one transformed packet of data to thereby generate a representation of the at least one packet of data.

7. A system according to Claim 6, wherein the first security gateway is capable of providing at least one security policy, wherein each security policy includes an application instance identifier associated with a security service, wherein the first security gateway is also capable of creating at least one security association, and wherein the first security gateway is capable of creating the at least one security association based upon the security service associated with the application instance identifier to thereby create a centralized key store including the at least one security policy and the at least one security association.

8. A system according to Claim 7, wherein the first security gateway is capable of providing at least one security policy further including at least one selector field having at least one selector value in a format common to a plurality of security service protocols, and wherein the first security gateway is capable of applying the security service further based upon the at least one security policy including the at least one selector value.

9. A system according to Claim 6, wherein the second security gateway is

capable of receiving the at least one transformed packet of data from the first security gateway, and thereafter applying the security service to the transformed at least one packet based upon the at least one security association.

10. A system according to Claim 6, wherein the first security gateway is capable of creating at least one security association according to an Internet Key Exchange (IKE) technique.

11. A security gateway for creating and maintaining a centralized key store comprising:

a security policy database capable of storing at least one security policy, wherein each security policy includes an application instance identifier associated with a security service;

a security association database capable of storing at least one security association; and

a processor capable of creating at least one security association based upon the security service associated with the application instance identifier to thereby create a centralized key store including the at least one security policy and the at least one security association.

12. A security gateway according to Claim 11, wherein the processor is capable of receiving at least one packet of data, and thereafter applying the security service associated with the application instance identifier to the at least one packet of data to thereby transform the at least one packet of data, and wherein the processor is capable of applying the security service to the at least one packet based upon the at least one security policy and the at least one security association.

13. A security gateway according to Claim 12, wherein the security policy database is capable of storing at least one security policy further including at least one selector field having at least one selector value in a format common to a plurality of security service protocols, and wherein the processor is capable of applying the security

service further based upon the at least one security policy including the at least one selector value.

14. A security gateway according to Claim 11, wherein the processor is also capable of receiving at least one transformed packet of data, and thereafter applying the security service associated with the application instance identifier to the at least one transformed packet of data to thereby generate a representation of the at least one packet of data, and wherein the processor is capable of applying the security service to the transformed at least one packet based upon at least one security association.

15. A security gateway according to Claim 11, wherein the processor is capable of creating at least one security association according to an Internet Key Exchange (IKE) technique.

16. A computer program product for creating and maintaining a centralized key store, the computer program product comprising a computer-readable storage medium having computer-readable program code portions stored therein, the computer-readable program portions comprising:

a first executable portion for providing at least one security policy, wherein each security policy includes an application instance identifier associated with a security service; and

a second executable portion for creating at least one security association, wherein the at least one security association is created based upon the security service associated with the application instance identifier to thereby create a centralized key store including the at least one security policy and at least one security association.

17. A computer program product according to Claim 16 further comprising:

a third executable portion for receiving at least one packet of data; and

a fourth executable portion for applying the security service associated with the application instance identifier to the at least one packet of data to thereby transform the at least one packet of data, wherein the security service is applied to the at least one packet

based upon the at least one security policy and the at least one security association.

18. A computer program product according to Claim 17, wherein the first executable portion provides at least one security policy further including at least one selector field having at least one selector value in a format common to a plurality of security service protocols, and wherein the fourth executable portion applies the security service further based upon the at least one security policy including the at least one selector value.

19. A computer program product according to Claim 16 further comprising:

a third executable portion for receiving at least one transformed packet of data; and

a fourth executable portion for applying the security service associated with the application instance identifier to the at least one transformed packet of data to thereby generate a representation of the at least one packet of data, wherein the security service is applied to the transformed at least one packet based upon the at least one security association.

20. A computer program product according to Claim 16, wherein the second executable portion creates at least one security association according to an Internet Key Exchange (IKE) technique.